UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/787,648	03/20/2001	Gerrit Roelofsen	PTT-111(4025	5973

7265 7590 12/01/2004

MICHAELSON AND WALLACE
PARKWAY 109 OFFICE CENTER
328 NEWMAN SPRINGS RD
P O BOX 8489
RED BANK, NJ 07701

EXAMINER	
DERWICH, KRISTIN M	
ART UNIT	**PAPER NUMBER**
2132	

DATE MAILED: 12/01/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/787,648	ROELOFSEN ET AL.	
	Examiner	Art Unit	
	Kristin Derwich	2132	

-- Th MAILING DATE of this c mmunication appears on the cover sheet with the correspondence address --

Period f r Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *3/20/2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-25* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-25* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *20 March 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☒ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *3/20/2001*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-25 pending.

Priority

2. Acknowledgement is made of applicant's claim for foreign priority under 35 U.S.C. 119(a)-(d).

Specification

3. The abstract of the disclosure is objected to because the form and legal phraseology often used in patent claims, such as "means" and "said," should be avoided. The abstract should describe the disclosure sufficiently to assist readers in deciding whether there is a need for consulting the full patent text for details. Correction is required in line 5 of the abstract where the legal phrase "said" is used. See MPEP § 608.01(b).

4. The disclosure is objected to because of the following informalities:

The specification has not been reviewed extensively for spelling and grammatical errors. It is requested that the applicant do a thorough review of the document and fix any spelling or grammatical errors.

On page 1, line 27, U.S. Patent Number 5,745,577 was cited as, "US-A-5745577". When a U.S. patent is cited for the first time it should be explicitly written as it appears above in order to avoid any confusion. Then any subsequent reference to the patent can be cited in an abbreviated fashion.

On page 1, line 42, the applicant states, "(see page 1 lines 32-34)" and it is unclear what the applicant is referring to since the subject matter represented by the citation is not relevant to the subject matter being presented in line 42.

On page 2, at line 42, the sentence is incomplete and not continued on the next page.

Appropriate correction is required.

Claim Rejections – 35 USC 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

5. Claim 1 recites the limitation "...in order to mask the values (K; D) used in the process (P)" in lines 8-9. There is insufficient antecedent basis for this limitation in the claim because D is not mentioned previously and not used in any of the figures.

6. Claims 8, 10, 11, 14-16 rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Claim 8 states the method consists of several steps, each step having one cryptographic function from the selection of F_i, F_i', F_i''. The dependent claims begin to select a specific function that could be different from the one previously chosen above. If F_i is chosen as the cryptographic function of claim 8, then a problem arises when claim 10 is reached and states, "Method according to claim 8, wherein the right-hand data (RD_i) is combined, in each step (S_i) and prior to the operation (F_i'), with the primary auxiliary value (A_i) of said step (S_i)." It is not clear if the

applicant intends for the right-hand data to be combined before the specific operation of F_i' and only F_i', or if it should be assumed that whichever operation was chosen in claim 8 should be inserted instead.

As it is currently stated in claim 10, it is assumed that the applicant is claiming a specific embodiment where the right-hand data (RD_i) is combined in each step (S_i) prior *only* to the operation (F_i'). The subsequent claims listed above induce the same confusion as claim 10 since the operation F_i' and F_i are used interchangeably.

7. Regarding claim 22, line 2, the word "preferably" renders the claim indefinite because it is unclear whether the limitation, "triple DES", following the word is part of the claimed invention. See MPEP § 2173.05(d).

8. Any claim not specifically addressed is rejected by virtue of its dependency.

Claim Rejections – 35 USC 102

9. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

9-1. Claims 1, 2, 7 and 8 are rejected under 35 U.S.C. 102(b) as being anticipated by Miyano (U.S. 5,442,705).

Miyano discloses a cryptographic system comprising:

As per claim 1:

Feeding, to a cryptographic process (P), values, namely the data (X) and a key (K), and carrying out the process (P) in order to form cryptographically processed output data (Y) (figure 1, where the Plaintext represents the data (X), Ciphertext represents the processed output (Y), Initial Key represents the key (K), and blocks R_0- R_{16} collectively represent the cryptographic process (P));

Characterized by feeding, to the process (P), auxiliary values (K*; A, B) and compensating, by an auxiliary process, the influence of the auxiliary values to the output data, in order to mask the values (K; D) used in the process (P) (figure 1, where K_1- K_{16} represent auxiliary values, the Key Scheduling Section represents the auxiliary process).

Miyano does not mention the terms "compensating", "auxiliary" or "mask" in his invention. Unless applicant can further define these terms as they pertain to the invention, the key schedule compensates the influence of the auxiliary values K_1- K_{16} by making the entire cryptographic process more secure. In addition, the key schedule masks the initial key.

As per claim 2:

An auxiliary value comprises a supplementary key (K*) which is fed to a supplementary process (P*) in order to form the key (K) (column 2, lines 65-66; column 3, lines 47-49, figure 1). Miyano does not mention the term "supplementary" in his invention but supplementary is defined as something added to complete a thing, make up for a deficiency, or extend or strengthen the whole. Since the key schedule

strengthens the security of the system as a whole it is considered a supplementary process, while a key is fed to the key schedule and the keys, K_1- K_{16} are produced which act as auxiliary values to the primary process.

As per claim 7:

The process (P) and the supplementary process (P*) each are built up from a number of steps, and wherein steps of the process (P) and the supplementary process (P*) are alternated (column 1, lines 64-68-column 2, lines 1-2; figure 1). The process (P) is represented by the steps R_0- R_{16} and alternate with the key schedule process which represents (P*). The two processes alternate since a new auxiliary key must be produced by the key schedule before the next R_i is executed.

As per claim 20:

According to the method of claim 8, combining is carried out using an XOR operation (Figure 3, column 4, lines 6-9). It can be seen in figure 3 that, as stated in claim 8, the right-handed data, R_n, goes through the cipher function and then that processed data goes to the combinatory XOR operation EX_n' which also takes the left-handed data, L_n as its other input.

As per claim 22:

The process (P) comprises DES, preferably triple DES (column 2, lines 47-53). As stated in Miyano, the invention is being discussed in connection with DES, this is exemplary and not limited to DES, meaning, triple DES could also be considered if it were preferred.

Any claim not specifically addressed is rejected by virtue of its dependency.

Claim Rejections – 35 USC 103

10. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

10-1. Claim 5 rejected under 35 U.S.C. 103(a) as being unpatentable over Miyano (U.S. 5,442,705) as applied to claim 1 above, and further in view of Schneier, *Applied Cryptography*.

Miyano fails to teach the data (X) being fed to the supplementary process (P*) in addition to the auxiliary key (K*). However, Schneier discloses a process called whitening where the supplementary process is an XOR combinatory process and both the data and some key material are fed to the XOR process before executing the primary process, in this case, DES (Schneier, 15.6).

It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to feed the data and the key to a supplementary XOR process in order to hide plaintext patterns, which is similar to masking, as stated in Schneier (pg 363).

10-2. Claim 8 rejected under 35 U.S.C. 103(a) as being unpatentable over Miyano (U.S. 5,442,705) as applied to claim 1 above, and further in view of Rivest (U.S. 5,724,428).

Miyano discloses a cryptographic process comprising:

A process (P) comprised of a number of steps (Si) (column 1, line 68-column 2, lines 1-2, figure 1). Here, stages are substituted for applicant's steps in view of *Roget's New Millenium Thesaurus, First Edition*, where step and stage are synonymous.

Each step having a cryptographic operation (Fi, Fi', Fi") for processing right-hand data (RD_i) derived from the data (X) (column 4, lines 6-9);

A combinatory operation (C_1) for combining with left-hand data (LD_i) also derived from the data (X), the processed right-hand data (FD_i) in order to form modified left data (SD_i) (figure 3). The combinatory operation (C_1) is represented by the EX_n' in figure 3 which takes the modified right-handed data from the cipher function and XOR's it with the left-handed data L_n.

Miyano fails to teach the right-hand data (RD_1) combined with a primary auxiliary value (A_1) prior to the first step (S_1) and the left-hand data (LD_1) combined with an additional auxiliary value (A_0). However, Rivest discloses a cryptographic algorithm that, initially, adds auxiliary values S[0] and S[1] to data (A) and (B) respectively before going into the block encryption process where S[0] , S[1] represent (A_1), (A_0) and (A), (B) represent (LD_1), (RD_1) (column 6, lines 16-19, figure 1B, column 10, lines 7-11).

It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to combine the right and left hand data with primary auxiliary values prior to the first step in order to make it difficult to determine the key (K) from (S) which is similar to a mask, and to assure that each round acts in a potentially different manner as stated in Rivest (column 5, lines 63-64; column 6, lines 18-19).

10-3. Claims 21, 23, 24 and 25 rejected under 35 U.S.C. 103(a) as being unpatentable over Miyano (U.S. 5,442,705) as applied to claim 1 above, and further in view of Bouricius et al. (U.S. 4,302,810).

Miyano fails to teach a method wherein the data (X) comprises identification data of a payment means (1) and the processed data (Y) forms a diversified key. Miyano also fails to teach a circuit for carrying out the method according to claim 1, a payment card provided with a circuit according to claim 23, and a payment terminal provided with a circuit according to claim 23. However, Bouricius et al. disclose a system which includes the secure transmission to a host machine of a transaction message which describes a financial transaction between a person and a retailer (column 3, lines 53-57), means for an encryption circuit to carryout the encryption processes (column 5, lines 37-39), an electronic funds transfer card (column 2, line 26) and a portable transaction terminal device (column 2, line 27).

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to use identification data of a payment means to produce a diversified key in addition to using a circuit to carryout a cryptographic method, a payment card and a payment terminal in order to prevent eavesdroppers on the transmission line from obtaining any information which could later be used for fraudulent, illegal, or any other purposes as stated by Bouricius et al. (column 2, lines 8-12).

Conclusion

11. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kristin Derwich whose telephone number is 571-272-7958. The examiner can normally be reached on Monday-Friday, 8:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

KMD

THOMAS R. PEESO
PRIMARY EXAMINER